Amendment to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) ~~Method~~ A method for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol, wherein said wireless communication apparatus has memory means including a separate unit comprising information to control the access of the wireless communication apparatus through a wireless communication network connected to said data communication apparatus, comprising ~~the following steps~~:

connecting said wireless communication apparatus to the separate unit, accessing the wireless communication network connected to said data communication ~~apparatus~~apparatus;

the wireless communication apparatus transmits a request to the data communication apparatus to establish a connection, said request comprising information of which at least one pre-defined ~~algorithm(s)~~ algorithm the wireless communication apparatus ~~supports,~~supports;

upon reception of said request, the data communication apparatus chooses at least one algorithm associated with a public and a private key, and transmits a message back to the wireless communication apparatus, said message comprising

the public key and information about which algorithm the data communication apparatus has ~~chosen,~~chosen;

upon reception of the message, comprising the public key, the wireless communication apparatus generates a master secret code, and calculates a signature based on the chosen algorithm, the public key and the master secret code, and transmits a response to the data communication apparatus, said response comprising the calculated ~~signature,~~signature;

upon reception of the ~~respond~~ response comprising the signature, the data communication apparatus calculates the master secret code based on the chosen algorithm, the signature received and the private key, and ~~establish~~ establishes a secure connection to the wireless communication apparatus, and ~~saving~~ saves said master secret code on said memory means and in the data communication apparatus, in order to re-establish the connection between the wireless communication apparatus and the separate unit at a later occasion.

2. (currently amended) A method according to claim 1, ~~and comprising~~ comprising ~~a step of~~ saving said master secret under a pre-defined time.

3. (currently amended) A method according to claim 1, further comprising ~~a step of~~ re-establishing the connection by transmitting a request from the wireless communication apparatus to the data communication apparatus, said request comprising the calculated signature based on the chosen algorithm, the public key

and the stored secret key, and upon reception of the request, the data communication apparatus calculates the master secret code based on the chosen algorithm, the signature received, and the private key, and, ~~establish~~ establishes a secure connection to the wireless communication apparatus.

4. (currently amended) A method according to claim 1, ~~and~~ comprising ~~a step of~~ providing said ~~separate unit in~~ memory means as a smart card.

5. (currently amended) ~~Wireless~~ A wireless communication apparatus for establishing a secure connection to a data communication apparatus based on a wireless application protocol, said wireless communication apparatus comprising:

communication means for establishing a connection to a wireless communication network connected to said data communication apparatus, memory means including a separate unit provided with information to control the access of the data communication apparatus through the wireless communication ~~network,~~network;

means for generating a master secret ~~code~~code;

control means arranged to use ~~a~~ at least one pre-defined algorithm(s) for generating a signature based on said master secret code and a public key received from said data communication apparatus, for use when the wireless communication apparatus establishes a secure connection to the data communication ~~apparatus,~~apparatus; and

said memory means ~~comprising~~ comprises a secure database for storing at least one master secret code ~~and/or~~ and at least one signature related to one or more data communication apparatus, in order to re-establish a secure connection to a data communication apparatus.

6. (currently amended) A wireless communication apparatus according to claim 5, ~~having its~~ wherein the memory ~~means~~ means is exchangeable.

7. (currently amended) ~~Wireless~~ A wireless communication apparatus according to claim 5 wherein the master secret code is stored on the separate unit.

8. (currently amended) ~~Wireless~~ A wireless communication apparatus according to any one of claims 5 to 7 wherein the signature is stored on the separate unit.

9. (currently amended) ~~Wireless~~ A wireless communication apparatus according to claim 5 wherein the master secret code is generated on the separate unit.

10. (currently amended) ~~Wireless~~ A wireless communication apparatus according to claim 5 wherein the signature is generated on the separate unit.

11. (currently amended) ~~Wireless~~ A wireless communication apparatus according to claim 5 wherein the separate unit comprises a smart card.

12. (original) An apparatus according to claim 11 wherein the smart card is a subscriber identity module.

13. (canceled)

14. (currently amended) A wireless communication apparatus according to claim 5 without a smart card.

15. (currently amended) ~~Memory~~ A memory card for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol, arranged to be connected to contact means, provided on said wireless communication apparatus, for providing information from the memory card to the wireless communication apparatus upon establishing a secure session to a data communication apparatus, said information is arranged to control the access of the data communication apparatus through a wireless communication network, and to save a calculated master secret related to one or more data communication apparatus, in order to re-establish a secure connection to a data communication apparatus.

16. (currently amended) A memory card according to claim 15, further comprising encryption means for encrypting the master secret, which is to be used as a signature for the wireless communication apparatus when ~~it~~ the wireless communication apparatus is establishing a secure connection.

17. (currently amended) A memory card according to claim 15, comprising a secure database provided with at least one ~~master~~ of a master secret code ~~and/or~~ and at least one signature related to at least one ~~or more~~ data communication apparatus, in order to re-establish a secure connection to data communication apparatus.

18. (previously presented) A memory card according to claim 15, provided on a smart card.

19. (currently amended) ~~System~~ A system for establishing a secure connection when using a wireless application protocol, comprising:

a data communication apparatus based on the wireless application ~~protocol,~~protocol;

a wireless communication network, connected to said data communication ~~apparatus,~~apparatus;

a wireless communication apparatus having memory means including a separate unit comprising information to control the access of the wireless

communication apparatus through the wireless communication ~~network,~~network;

wherein

the wireless communication apparatus is arranged to transmit a request to the data communication apparatus to establish a connection, said request comprising information of which at least one pre-defined ~~algorithm(s)~~ algorithm the wireless communication apparatus ~~supports,~~supports;

upon reception of said request, the data communication apparatus is arranged to choose at least one algorithm, associated with a public key and a private key, and to transmit a message back to the wireless communication apparatus, said message comprising the public key and information about which algorithm the data communication apparatus will ~~choose,~~choose;

upon reception of said message, comprising the public key, the wireless communication apparatus is arranged to generate a master secret code, to calculate a signature based on the chosen algorithm, the public key and the master secret code, and to transmit a ~~respond~~ response to the data communication apparatus, said ~~respond~~ response comprising the calculated ~~signature,~~signature;

upon reception of the ~~respond~~ response comprising the signature, the data communication apparatus is arranged to calculate the master secret code based on the chosen algorithm, the signature received, and the private key, ~~and, thus~~ to establish a secure connection to the wireless communication ~~apparatus,~~ apparatus; and

said memory means ~~being~~ is arranged to save said master secret code, in order to re-establish the connection at a later occasion.

20. (currently amended) A system according to claim 19, wherein said master secret is arranged to be saved under a pre-defined time.

21. (previously presented) A system according to claim 19, said memory means is a smart card.

22. (currently amended) A wireless communication apparatus for establishing a secure connection to a data communication apparatus through a wireless network based on a wireless application protocol, said wireless communication apparatus comprising:

means for establishing a connection with the data communication apparatus through the wireless ~~network~~network;

means for retrieving access information including which of a set of at least one ~~pre-define~~ pre-defined ~~algorithms~~ algorithm is supported, for transmission to the data communication apparatus;

means for processing information including a public key ~~and the~~ and selection of one of the at least one supported ~~algorithms~~ algorithm received from the data communication apparatus for storage;

means for retrieving a signature based on a generated master secret code and the public key received from the data communication apparatus; and

means for ~~utilising~~ utilizing at least one of the signature ~~and/or~~ and the master secret key during communication with the data communication apparatus in order to re-establish a secure connection.

23. (currently amended) A memory card for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol comprising contact means for cooperation with the wireless communication apparatus comprising:

a memory for storing a master secret code associated with the data communication apparatus and responsive to a request from the wireless communication apparatus to provide such code for ~~utilisation~~ utilization of the master secret key during communication with the data communication apparatus in order to re-establish a secure connection.

24. (currently amended) ~~Wireless~~ A wireless communication apparatus for establishing a secure connection to a data communication apparatus based on a wireless application protocol, said wireless communication apparatus comprising:

communication means for establishing a connection to a wireless communication network connected to said data communication ~~apparatus,~~apparatus;

memory means provided with information to control the access of the data communication apparatus through the wireless communication network upon establishing a secure session to a data communication ~~apparatus,~~apparatus;

reading means for reading information received from the data communication apparatus and the information provided on said memory ~~means,~~means;

means for generating a master secret ~~code,~~code;

control means arranged to use ~~a~~ at least one pre-defined ~~algorithm(s)~~ algorithm for generating a signature based on said master secret code and a public key received from said data communication apparatus, which is to be used when the wireless communication apparatus is going to establish a secure connection to the data communication ~~apparatus,~~ apparatus; and

said reading means comprising a secure database provided with at least one ~~master~~ a master secret code ~~and/or~~ and at least one signature related to at least one ~~or more~~ data communication apparatus, in order to re-establish a secure connection to a data communication apparatus.

25. (currently amended) A method according to claim 2, further comprising ~~a step of~~ re-establishing the connection by transmitting a request from the wireless communication apparatus to the data communication apparatus, said request comprising the calculated signature based on the chosen algorithm, the public key and the stored secret key, and upon reception of the request, the data communication apparatus calculates the master secret code based on the chosen

algorithm, the signature received, and the private key, and, ~~establish~~ establishes a secure connection to the wireless communication apparatus.

26. (currently amended) A method according to claim 2, ~~and~~ comprising ~~a step of~~ providing said ~~separate unit in~~ memory means as a smart card.

27. (currently amended) A method according to claim 3, ~~and~~ comprising ~~a step of~~ providing said ~~separate unit in~~ memory means as a smart card.

28. (currently amended) ~~Wireless~~ A wireless communication apparatus according to claim 6 wherein the master secret code is stored on the separate unit.

29. (currently amended) ~~Wireless~~ A wireless communication apparatus according to claim 6 wherein the master secret code is stored on the separate unit.

29. (currently amended) A wireless ~~Wireless~~ communication apparatus according to claim 6 wherein the master secret code is generated on the separate unit.

30. (currently amended) A wireless ~~Wireless~~ communication apparatus according to claim 7 wherein the master secret code is generated on the separate unit.

31. (currently amended) A wireless ~~Wireless~~ communication apparatus according to claim 8 wherein the master secret code is generated on the separate unit.

32. (currently amended) A wireless ~~Wireless~~ communication apparatus according to claim 6 wherein the signature is generated on the separate unit.

33. (currently amended) A wireless ~~Wireless~~ communication apparatus according to claim 7 wherein the signature is generated on the separate unit.

34. (currently amended) A wireless ~~Wireless~~ communication apparatus according to claim 8 wherein the signature is generated on a separate unit.

35. (currently amended) A wireless ~~Wireless~~ communication apparatus according to claim 9 wherein the signature is generated on the separate unit.

36. (currently amended) A wireless ~~Wireless~~ communication apparatus according to claim 6 wherein the separate unit comprises a smart card.

37. (currently amended) A wireless ~~Wireless~~ communication apparatus according to claim 7 wherein the separate unit comprises a smart card.

38. (currently amended) A wireless ~~Wireless~~ communication apparatus according to claim 8 wherein the separate unit comprises a smart card.

39. (currently amended) A wireless ~~Wireless~~ communication apparatus according to claim 9 wherein the separate unit comprises a smart card.

40. (currently amended) A wireless ~~Wireless~~ communication apparatus according to claim 10 wherein the separate unit comprises a smart card.

41. (canceled)

42. (currently amended) A memory card according to claim 16, comprising a secure database provided with at least one of a master secret code ~~and/or~~ and at least one signature related to at least one ~~or more~~ data communication apparatus, in order to re-establish a secure connection to data communication apparatus.

43. (previously presented) A memory card according to claim 16, is provided on a smart card.

44. (previously presented) A memory card according to claim 17, provided on a smart card.

45. (previously presented) A system according to claim 20, said memory means is a smart card.

46. (new) A wireless communication device for receiving therein a separate unit with memory means, the device being operable to establish a secure connection with a data communication apparatus based on a wireless application protocol through a wireless communication network, said wireless communication device comprising: communication means for establishing said connection with said data communication apparatus, electrical contact means for communicating information between the communication means and the separate unit, the device being configured so that when said separate unit is received therein the resulting combination is operable to:

generate a master secret code;

use a pre-defined algorithm to create a signature for use when the wireless communication device establishes a secure connection to the data communication apparatus, the signature being based on the master secret code and a public key received from said data communication apparatus; and

to store at least one of said at least one master secret code and at least one signature related to at least one data communication apparatus in the memory means of the separate unit to enable re-establishment of the secure connection on a later occasion.

47 (new) A wireless communication apparatus according to claim 46 operable when said separate unit is received therein to retrieve said at least one of at least one master secret code and at least one signature when re-establishing the secure connection on a later occasion.

48 (new) A wireless communication device according to claim 46 operable when said separate unit is received therein to cause both the generation and storage of the master secret code in the separate unit.

49. (new) A wireless communication device according to claim 47 operable when said separate unit is received therein to cause both the generation and storage of the master secret code in the separate unit.

50. (new) A wireless communication device according to claim 46 including a processor operable to generate the master secret code.

51. (new) A wireless communication device according to claim 47 including a processor operable to generate the master secret code.

52. (new) A wireless communication device according to claim 46 operable when said separate unit is received therein to cause the generation of the signature in the separate unit.

53. (new) A wireless communication device according to claim 47 operable when said separate unit is received therein to cause the generation of the signature in the separate unit.

54. (new) A wireless communication device according to claim 48 operable when said separate unit is received therein to cause the generation of the signature in the separate unit.

55. (new) A wireless communication device according to claim 49 operable when said separate unit is received therein to cause the generation of the signature in the separate unit.

56. (new) A wireless communication device according to claim 47 wherein the contact means are configured to receive the separate unit in the form of a smart card.

57. (new) A wireless communication device according to claim 48 wherein the contact means are configured to receive the separate unit in the form of a smart card.

58. (new) A wireless communication device according to claim 49 wherein the contact means are configured to receive the separate unit in the form of a smart card.

59. (new) A wireless communication device according to claim 50 wherein the contact means are configured to receive the separate unit in the form of a smart card.

60. (new) A wireless communication device according to claim 51 wherein the contact means are configured to receive the separate unit in the form of a smart card.

61. (new) A wireless communication device according to claim 52 wherein the contact means are configured to receive the separate unit in the form of a smart card.

62. (new) A wireless communication device according to claim 53 wherein the contact means are configured to receive the separate unit in the form of a smart card.

63. (new) A wireless communication device according to claim 54 wherein the contact means are configured to receive the separate unit in the form of a smart card.

64. (new) A wireless communication device according to claim 55 wherein the contact means are configured to receive the separate unit in the form of a smart card.

65. (new) A wireless communication device according to claim 46 wherein the contact means are configured to receive the separate unit in the form of a SIM card.

66. (new) A wireless communication device according to claim 46 wherein the contact means are configured to receive the separate unit in the form of a SIM card.

67. (new) A wireless communication device according to claim 47 wherein the contact means are configured to receive the separate unit in the form of a SIM card.

68. (new) A wireless communication device according to claim 48 wherein the contact means are configured to receive the separate unit in the form of a SIM card.